**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

| | |
|---|---|
| JOHN FINN, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>EMPRESS AMBULANCE SERVICES, INC., d/b/a EMPRESS EMS<br><br>Defendant. | Case No.<br><br>CLASS ACTION<br><br><br><br>JURY TRIAL DEMANDED |

## CLASS ACTION COMPLAINT

Plaintiff John Finn ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through his attorneys, brings this Class Action Complaint against Defendant Empress Ambulance Service, Inc. d/b/a Empress EMS ("Empress") and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

## INTRODUCTION

1. Plaintiff brings this class action against Empress for its failure to secure and safeguard his and approximately 318,558 other individuals' private and confidential information, including names, dates of service, Social Security numbers, and insurance information ("PII/PHI").

2. Defendant is a corporation in Yonkers, New York that provides Emergency Medical services and mutual aid to the neighboring communities.

3. On or about July 14, 2022, Empress discovered that unauthorized individuals had gained access to Empress's network systems and had access to the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. Empress owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Empress breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Empress's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all New York residents whose PII/PHI was exposed as a result of the Data Breach, which Empress learned of on or about July 14, 2022 and first publicly acknowledged on or about September 9, 2022.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations New York GBL § 349, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

## PARTIES

7. Plaintiff Finn is a New York resident. He provided his PII/PHI to Empress in connection with receiving health care services from Empress. He received a letter from Empress on or about September 18, 2022 notifying him that his PII/PHI may have been exposed in the Data Breach.

8. Defendant Empress EMS, Inc. is a corporation organized under the laws of New York and maintains its principal place of business at 722 Nepperhan Avenue, Yonkers, New York 10703.

## JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332 (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), and is a class action involving 100 or more class members. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. This Court has personal jurisdiction over Empress because Empress is a corporation organized under the laws of New York and has its principal place of business at 722 Nepperhan Ave, Yonkers, New York, 10703.

11. Venue properly lies in this judicial district pursuant to 28 U.S.C. § 1391 because, *inter alia,* the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this district; Defendant's principal place of business is in this district; Defendant transacts substantial business and has agents in this district; a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district; and because Plaintiff resides within this district.

## FACTUAL ALLEGATIONS

### *Overview of Empress*

12. Empress is a corporation that provides emergency medical services and after care transportation in New York state.

13. In the regular course of its business, Empress collects and maintains the PII/PHI of patients, former patients, and other persons to whom it is currently providing or previously provided health-related or other services.

14. Empress requires patients to provide personal information before it provides them services. That information includes, *inter alia*, names, addresses, dates of birth, health insurance information, and Social Security numbers. Empress stores this information digitally.

15. In their Privacy Notice, Empress states that it is "committed to protecting your personal health information" and that "We respect your privacy, and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times."[1]

16. Plaintiff and Class members are, or were, patients of Empress or received health-related or other services from Empress, and entrusted Empress with their PII/PHI.

***The Data Breach***

17. On or about July 14, 2022, Empress discovered that an unauthorized individual, or unauthorized individuals, gained access to Empress's network systems. Empress revealed that unknown parties first accessed Empress's computer networks on May 26, 2022 and copied files on July 13, 2022.

18. Empress began to notify patients about the data breach on or about September 9, 2022. The letter posted on Empress's website states that the information that was accessed

[1] Empress Emergency Medical Services, *Customer Service*, EMPRESSEMS.COM, http://empressems.com/files/empressprivacy.pdf (last visited Sept. 20, 2022).

included: "[P]atient names, dates of service, insurance information, and in some instances, Social Security numbers."[2]

***Empress Knew that Criminals Target PII/PHI***

19. At all relevant times, Empress knew, or should have known, its patients' PII/PHI was a target for malicious actors. Despite such knowledge, Empress failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that Empress should have anticipated and guarded against.

20. Cyber criminals seek out PII/PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.[3] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[4] In 2021, 905 health data breaches were reported and according to Protenus's assessment, and although a record number of data breaches were reported, the impact of breaches continues to be underreported overall, and underrepresented to the public.[5]

21. PII/PHI is a valuable property right.[6] The value of PII/PHI as a commodity is

---

[2] Empress Emergency Medical Services, *Security Incident*, EMPRESSEMS.COM, http://empressems.com/securitynotice.pdf (last visited Sept. 20, 2022).

[3] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Sept. 21, 2022).

[4] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Sept. 21, 2022).

[5] Protenus, 2022 Brach Barometer, PROTENUS.COM, https://www.protenus.com/resources/2022-breach-barometer (last accessed Sept. 21, 2022)

[6] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

measurable.[7] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[8] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[9] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

22. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

23. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[10] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[11] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority

---

7 *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

8 OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

9 IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

10 *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

11 *Id.*

of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[12]

24. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[13] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[14]

25. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[15] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[16]

26. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies

---

12 *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

13 SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

14 Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

15 *What Happens to Stolen Healthcare Data*, *supra* at n.10.

16 *Id.*

confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[17]

27. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

***Theft of PII/PHI Has Grave and Lasting Consequences for Victims***

28. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[18]

29. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[19] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card

---

17 Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

18 *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

19 The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[20]

30. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[21]

31. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[22]

32. Theft of SSNs, which are reportedly exposed in this breach, creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

---

[20] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[21] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Sept. 21, 2022).

[22] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Sept. 20, 2022).

33. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[23]

34. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[24] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[25] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[26] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[27]

35. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These

---

[23] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[24] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf

[25] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.14.

[26] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Sept. 20, 2022).

[27] *Id*.

changes can affect the healthcare a person receives if the errors are not caught and corrected.

- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[28]

36. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[29]

37. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

---

[28] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 24.

[29] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

***Damages Sustained by Plaintiff and the Other Class Members***

38. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

## CLASS ALLEGATIONS

39. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b).

40. Plaintiff brings this action on behalf of themselves and all members of the following Class of similarly situated persons:

> All persons whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach, including all persons who were sent a notice of the Data Breach.

41. Excluded from the Class is Empress and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

42. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

43. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Empress reported to the U.S. Department of Health and

Human Services' Office of Civil Rights that approximately 318,558 individuals' information was exposed in the Data Breach.

44. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Empress had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether Empress failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;

c. Whether an implied contract existed between Class members and Empress providing that Empress would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

d. Whether Empress breached its duties to protect Plaintiff's and Class members' PII/PHI; and

e. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

45. Empress engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

46. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Empress, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

47. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

48. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Empress, so it would be impracticable for Class members to individually seek redress from Empress's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## CAUSES OF ACTION

## COUNT I

## NEGLIGENCE

49. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

50. Empress owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

51. Empress knew the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Empress knew of the many data breaches that targeted healthcare providers in recent years.

52. Given the nature of Empress's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Empress should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

53. Empress breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

54. It was reasonably foreseeable to Empress that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would

result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

55. But for Empress's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

56. As a result of Empress's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

## COUNT II

## NEGLIGENCE PER SE

57. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

58. Empress's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

59. Empress's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Empress, of failing to employ reasonable measures to protect and secure PII/PHI.

60. Empress violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. Empress's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

61. Empress's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

62. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

63. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

64. It was reasonably foreseeable to Empress that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

65. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Empress's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

## COUNT III

## BREACH OF FIDUCIARY DUTY

66. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

67. Plaintiff and Class members gave Empress their PII/PHI in confidence, believing that Empress would protect that information. Plaintiff and Class members would not have provided Empress with this information had they known it would not be adequately protected. Empress's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Empress and Plaintiff and Class members. In light of this relationship, Empress must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

68. Empress has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly

protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

69. As a direct and proximate result of Empress's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Empress's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

## COUNT IV

## BREACH OF IMPLIED CONTRACT

70. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

71. In connection with receiving medical services, Plaintiff and all other Class members entered into implied contracts with Empress.

72. Pursuant to these implied contracts, Plaintiff and Class members paid money to Empress, whether directly or through their insurers, and provided Empress with their PII/PHI. In exchange, Empress agreed to, among other things, and Plaintiff understood that Empress would: (1) provide medical services to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect

Plaintiff's and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

73. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Empress, on the other hand. Indeed, as set forth *supra*, Empress recognized the importance of data security and the privacy of its patients' PII/PHI in its Privacy Notice. Had Plaintiff and Class members known that Empress would not adequately protect its patients' and former patients' PII/PHI, they would not have received medical services from Empress.

74. Plaintiff and Class members performed their obligations under the implied contract when they provided Empress with their PII/PHI and paid—directly or through their insurers—for health care services from Empress.

75. Empress breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

76. Empress's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

77. Plaintiff and all other Class members were damaged by Empress's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they

are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

## COUNT V

## UNJUST ENRICHMENT

78. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

79. This claim is pleaded in the alternative to the breach of implied contract claim.

80. Plaintiff and Class members conferred a monetary benefit upon Empress in the form of monies paid for healthcare services or other services.

81. Empress accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Empress also benefitted from the receipt of Plaintiff's and Class members' PHI, as this was used to facilitate payment.

82. As a result of Empress's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

83. Empress should not be permitted to retain the money belonging to Plaintiff and Class members because Empress failed to adequately implement the data privacy and security

procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

84. Empress should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

## COUNT VI

## VIOLATIONS OF THE NEW YORK DECEPTIVE ACTS AND PRACTICES ACT N.Y. Gen. Bus. Law § 349 ("GBL")

85. Plaintiffs re-allege and incorporate by reference the preceding paragraphs.

86. Plaintiff Finn and New York Class members are "persons" within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(h).

87. Empress is a "person, firm, corporation or association or agent or employee thereof" within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(b).

88. Under GBL section 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce" are unlawful.

89. Empress violated the GBL through its promise to protect and subsequent failure to adequately safeguard and maintain Plaintiff and Class members' PII/PHI. Empress failed to notify Plaintiff and other class members that, contrary to its representations about valuing data security and privacy, it does not maintain adequate controls to protect PII/PHI. It omitted all of this information from Plaintiff and class members.

90. As a result of Empress's above-described conduct, Plaintiff and the Class have suffered damages from the disclosure of their information to unauthorized individuals.

91. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Empress's violations of the GBL. Plaintiff and Class members have

suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

92. Plaintiff Finn, individually and on behalf of the New York Class, requests that this Court enter such orders or judgments as may be necessary to enjoin Empress from continuing its unfair and deceptive practices.

93. Under the GBL, Plaintiff and Class members are entitled to recover their actual damages or $50, whichever is greater. Additionally, because Defendant acted willfully or knowingly, Plaintiff Finn and New York Class members are entitled to recover three times their actual damages. Plaintiff Finn also is entitled to reasonable attorneys' fees.

## PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against Empress as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Empress from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: September 22, 2022

Respectfully submitted,

*/s/ Tina Wolfson*

TINA WOLFSON (NY Bar # 5436043)
*twolfson@ahdootwolfson.com*
DEBORAH DE VILLA (NY Bar # 5724315)
*ddevilla@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH*
*aferich@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

*Attorneys for Plaintiff*

**pro hac vice* to be submitted